Statement of Daniel Burton

Vice President of Government Affairs

Entrust, Inc.

Before

The House Energy and Commerce Committee

Subcommittee on Commerce, Trade and Consumer Protection

"**Securing Consumers' Data: Options Following Security Breaches"**

May 11, 2005

Good Morning. Chairman Stearns and distinguished Members of the Subcommittee, thank you for holding this hearing and giving me the opportunity to provide testimony on this important subject. My name is Daniel Burton, and I am Vice President of Government Affairs for Entrust, Inc. In my testimony today, I will discuss the impact of security breaches and what we can do about them.

Entrust is a world leader in securing digital identities and information. As a security software company, we are in the business of protecting our customers – and by extension your constituents – with proven technology solutions that secure digital information. Over 1,200 enterprises and government agencies in more than 50 countries, including the US Department of Treasury, the Department of Justice and numerous nuclear laboratories, rely on Entrust software, so we have a lot of experience in this field. Entrust provides software solutions that protect your digital identity through authentication, enforce policy through advanced content scanning, and protect your information assets through encryption. Our mission is to work with customers to put in place the technologies, policies and procedures necessary to protect digital identities and information.

I would like to note with appreciation this committee's longstanding interest in on-line privacy. As a company that is on the front lines of the daily battle to protect sensitive information, Entrust applauds your activities and encourages your continued leadership in this area. You have followed this issue closely for several years and built up considerable

expertise. As a result, you are well positioned to play a critical role in protecting the privacy of individuals, companies and governments.

The privacy issues we are facing today are very different than they were a few years ago. Then, much of the debate revolved around limited "opt-in" and "opt-out" provisions that determined what kind of consent was necessary to share personal information for marketing purposes. Today, with rampant theft of confidential personal information a reality, the Internet privacy debate is focused on squarely on security.

Crime on the Net

This shift in emphasis – from nuisance to outright crime – represents a sea change for public policy. For years we have enjoyed the productivity improvements that networked computing afforded and learned to live with the nuisances that came with it. We may have been concerned about hacking for "honor" and other pranks, but like early version of spam, viruses and unsolicited marketing campaigns, we tolerated them as a small price to pay for the extraordinary dividends the Internet provided. Today, these nuisances are overshadowed by a much more sinister problem – organized crime.

Just like companies and governments, criminals have come to realize that the Internet is a powerful business tool. As mountains of sensitive personal, corporate and government information have moved onto the net, crime has too. For criminals, gaining access to names, addresses, credit card information, social security numbers and other identifiers is a gateway to ready cash. As a result, computer hackers no longer fit the profile of pimply

faced teenagers who lose interest as soon as they get a girlfriend. Increasingly, they are skilled criminals who have a sophisticated business plan, mount wholesale attacks, move quickly around the globe and cover their tracks. Our understanding of these crimes and the role of law enforcement is still evolving, but the stakes are high. If Internet crime causes American consumers to retreat from online transactions, U.S. business and government will suffer huge productivity reversals that could cripple not only e-commerce, but also the economy at large.

The statistics are staggering. The Federal Trade Commission estimates that 9-10 million Americans are victims of identity theft per year. Total cost to business and consumers is approaching $50 billion. Almost 2 million US adult Internet users had their identities stolen in 2004. Almost 12% of the fraud is online.

As a result, the public temperature is rising. A January 2005 IDC Survey showed that close to 60% of US consumers are concerned about identity theft, and almost 6% have taken the remarkable step of switching banks as a result. A survey that Entrust conducted reaffirmed this concern. It found that 80% of individuals are worried about someone stealing their on-line identity and using it to access their on-line bank accounts.

The underlying question of this hearing is whether we are doing enough to protect confidential information. The answer, unfortunately, is that as a nation we are not prepared to deal with the reality of cybercrime. The necessary legal framework to

safeguard consumers and companies is still incomplete; enforcement efforts and resources are inadequate; and much of the private sector is still in denial.

Bigger than Banks, Hospitals and Data Brokers

The identity theft crisis extends well beyond regulated industries like banking and healthcare that many people view as guardians of their sensitive information. It's even bigger than data brokers, despite all the attention they have received lately. The breaches at Bank of America, Choicepoint and Lexis-Nexis may have sparked public outrage about identity theft, but you only have to look at the kinds of organizations that have announced breaches in recent months to understand that the problem goes much deeper. Discount Shoe Warehouse, Paymaxx, the San Jose Medical Group, the University of California at Berkeley, George Mason University, SAIC, Time Warner – none of these are data brokers, yet they all suffered breaches of highly sensitive personal information. The scope of these breaches demonstrates that the universe of organizations holding sensitive personal information is quite large. Focusing remedies exclusively on data brokers is like protecting your home from burglars by locking the front door and leaving all the windows wide open. It may make you feel better, but it won't do much to prevent a robbery. Similarly, passing a law that requires only data brokers to issue notifications when their systems are breached will do nothing to safeguard the mountains of personal information that are held by other organizations. True success lies in a much broader approach.

It is for this reason that the recent state breach notification laws we see around the country are not limited to banks, healthcare providers and data brokers. It may interest you to know that many of the most proactive states in this arena are represented by members of this Committee. For example, California was the first state to pass such a bill (H.B. 1386). It took effect on July 1, 2003 and requires a state agency, person or business that conducts business in California, and that owns or licenses computerized data that includes personal information to disclose breaches of unencrypted personal information to California residents. Arkansas has also passed a disclosure law (Senate Bill 1167) that covers "individuals, businesses and state agencies that acquire, own or license personal information about the citizens of the State of Arkansas . . ." Florida has a bill (H.B. 481) awaiting the Governor's signature that covers "Any person who conducts business in this state and maintains computerized data in a system that includes personal information . . ." In all, over twenty states have introduced such legislation, and there is a possibility that we could have over a dozen competing and conflicting state breach notification laws in effect by this summer.

Given this backdrop of crime, systematic breaches and proliferating state legislation, Congress needs to act.

Technology and Public Policy

In trying to determine what role Congress should play, it is important to understand some of the key technologies underlying information security. I will focus on two: confidentiality and authentication. Confidentiality means assuring that information is not

disclosed to unauthorized persons. Encryption -- which is the coding or scrambling of information so that it can only be decoded and read by someone with the correct decoding key -- is the technology often associated with confidentiality. Encryption comes in different strengths. Many of the state breach notification bills make specific reference to it.

Data in transit, such as e-mail, presents different encryption challenges than stored data. And since stored data is held in a variety of repositories, from mainframes to laptops, and in different ways, such as data bases and directories, it presents unique encryption challenges of its own. Software applications and data bases are typically built for speed, not security, so the issue is not just whether to encrypt them, but how and where to apply it. Not all data must be encrypted, but there is an increasing demand to encrypt sensitive personal data, even if it affects performance.

Authentication means corroborating that a user is who they claim to be. It is often linked closely with authorization, which means that you have the right to access the information in question. Authentication technologies include user name and password (referred to as first factor since they relate to something you know) and physical tokens with secret codes (referred to as second factor since they are something you have). An even stronger form of authentication technology is the digital certificate, which is an electronic identifier that establishes your credentials. Digital certificates are issued by a certification authority. They contain your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital

signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Using public key cryptography and digital certificates, the sender can assure that only the intended recipient can open the message, and the recipient knows that only the authorized sender could have sent the message.

Much of the public policy debate about identity theft has focused on the need to authenticate consumer identities. Just as important, however, is the need to authenticate employer and supplier identities at both ends of a transaction. Since many breaches are internal, proper authentication of the employees, customers and partners who have privileged access to information is critical to preventing identity theft.

The Need for Additional Legislative Safeguards

There has been a lot of discussion about whether existing law is sufficient to prevent identity theft. Although industry at large has traditionally opposed federal legislation in this area, rampant identity theft, the proliferation of security breaches, and the passage of state breach notification laws have caused many companies to change their view. Entrust believes that additional Federal legislation could assist holders of sensitive personal information in their efforts to prevent consumer fraud and identity theft. Specifically, we believe that the following measures deserve consideration.

1. Establish a uniform national breach notification policy for unauthorized access to unencrypted personal information.

Breach notification laws are necessary to inform consumers when their sensitive personal information has been compromised so that they can guard themselves against identity crimes. As mentioned above, several states have passed breach notification laws and many more have introduced this legislation. A uniform national notification standard is needed to preempt conflicting state laws and establish consistent requirements. In weighing such a provision, Congress should keep in mind two important criteria that are enshrined in state law.

First, the notification requirement should apply to **all entities that hold sensitive personal information**. Confidential information is held by a wide variety of institutions, including employers, retailers, lawyers and government agencies. If the Federal notification requirement is limited to data brokers and regulated industries like banking and health-care, none of these other organizations will be covered. If this were the case, organizations like SAIC, Time Warner, George Mason University and Discount Shoe Warehouse -- all of whom have suffered breaches and sent out notifications in recent months -- would not be required by Federal law to notify those people whose identities had been compromised.

Second, and just as important, if the personal **information is appropriately encrypted, notification should not be required.** The reason for this provision is that unauthorized access to encrypted data reveals only scrambled code that is meaningless. For example, if the personal information of the 600,000 current and former employees of Time Warner had been encrypted on the tapes that were lost, there would have been very little risk of

identity theft because the information would have been unintelligible to anyone without the proper access.

There are several different kinds of encryption, however, not all of which are reliable. To insure that the encryption is adequate, Congress should insist on the encryption standards developed by the National Institute of Standards and Technology. Organizations that suffer breaches should not have to issue notifications if their *data, whether in storage or in transit, is encrypted with a NIST approved encryption algorithm, uses NIST approved key management techniques and has cryptographic operations performed within a FIPS 140 validated cryptographic module.*

2. Require second factor authentication for access to sensitive personal information.

The Federal Deposit Insurance Corporation (FDIC) issued a thorough study of identity theft in its December 2004 report, Putting an End to Account-Hijacking Identity Theft. The FDIC's lead recommendation is "Upgrading existing password-based single-factor customer authentication systems to two-factor authentication." Industry analysts have confirmed this view. Jonathan Penn, an analyst at Forrester, has written that "In response to consumers' rising concerns about fraud and identity theft, many organizations are evaluating strong authentication solutions . . ." And John Pescatore, an analyst with Gartner, has written "When you get to the core issue of most identity theft attacks, it really falls back to needing stronger authentication . . ."

The problem with two-factor authentication is that, until recently, it was difficult to administer and prohibitively expensive to implement on a large scale. Fortunately, new technology breakthroughs by Entrust and others have substantially reduced the cost and complexity associated with two factor authentication. These breakthroughs should facilitate the broader use of this technology to organizations that must safeguard large quantities of digital identities.

3. Encourage enterprises that hold sensitive personal information to use technological and other means to assure compliance with their privacy policies. Since the majority of breaches come from insiders, one way to limit them is for organizations to screen communications for privacy violations. The FDIC has already highlighted this imperative in its safeguards guidance to financial institutions, recommending that they establish controls to prevent employees from providing customer information to unauthorized individuals. Since banks are not the only ones holding sensitive personal information, these controls should be extended to non-financial institutions as well.

Because the majority of electronic data is at some point associated with e-mail, controls that assure outgoing e-mail communications and attachments comply with privacy policies can help reduce identity theft. To the extent that organizations monitor e-mail traffic at all, however, many rely on a manual review of only a small sample of e-mail traffic. Fortunately, technology now exists that has automated compliance controls capable of blocking, archiving, redirecting or securing e-mail communications in real-

time. Enterprises that are in the business of holding sensitive personal information should be encouraged to consider adopting it.

4. Extend security requirements similar to the Gramm-Leach-Bliley Act safeguards for financial institutions to all entities that retain sensitive personal information. This Subcommittee should consider extending the risk management, reporting and accountability requirements documented in FDIC and FTC safeguards guidance to all enterprises that hold sensitive personal information. Title V of the Gramm-Leach-Bliley Act (GLBA) states that financial institutions must establish safeguards for customer records and information. In her testimony before this Subcommittee on March 15, 2005, the Chair of the Federal Trade Commission, Deborah Majoras, noted that to the extent that data brokers fall within the GLBA definition of financial institutions they must abide by these safeguards. As discussed earlier, however, limiting the extension of the GLBA safeguards only to data brokers would overlook the vast numbers of other organizations that hold sensitive personal information and do little to stem the tide of identity theft.

Since any discussion of security safeguards raises questions about technology mandates, it is important to emphasize that the regulatory guidance for implementing the GLBA safeguards addresses such issues as the need to develop a written security plan, to designate appropriate personnel to oversee it, and to conduct a risk assessment. None of these is a technology requirement. Instead, they relate to sound management practices. The National Cyber Security Summit Task Force on Information Security Governance that Entrust CEO Bill Conner co-chaired took a similar approach. In its April 2004

report, Information Security Governance: A Call to Action, it concluded that "The best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of Boards and CEOs." It recommended that CEOs have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to their board of directors. In addition, it emphasized the need for organizations to establish a security management structure to assign explicit individual roles, responsibility, authority and accountability.

Conclusion

This Subcommittee has an important role to play in the effort to secure personal data. The goal is clear. We should do everything we can to encourage holders of sensitive information to secure it from unauthorized access and, in the event of a breach, to notify individuals so that they can protect themselves. The reality of rampant identity theft is proof that we have no time to waste. The fact that sensitive personal information is held by a wide variety of organizations demonstrates that a narrow solution will be insufficient.

Information security is not only a technical issue, but also a governance challenge. Technology solutions, like encryption, strong authentication and automated e-mail compliance with privacy policies, can do a lot to prevent unauthorized access to personal information. But they must be grounded in the risk management, reporting and accountability that can only be implemented with the active engagement of executive management.